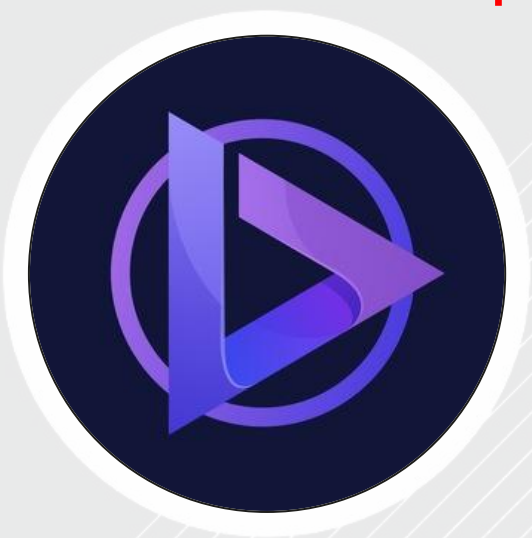
SPYWOLF

Security Audit Report

The contract is currently
deployed on TESTNET



Completed on

July 5, 2022

MADE IN USA 🇺🇸

SPYWOLF.CO @SPYWOLFNETWORK @SPYWOLFNETWORK

OVERVIEW

This audit has been prepared for **Cleeps** to review the main aspects of the project to help investors make make an informative decision during their research process.

You will find a a summarized review of the following key points:

- ✔ Contract's source code
- ✔ Owners' wallets
- ✔ Tokenomics
- ✔ Team transparency and goals
- ✔ Website's age, code, security and UX
- ✔ Whitepaper and roadmap
- ✔ Social media & online presence

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

Cleeps

PROJECT DESCRIPTION

According to the project Litepaper:

CLEEPS — is an innovative NFT marketplace for short videos, which offers you the most comfortable ways to find desired collection or token, and download your own in a blink of an eye. It will be made as a PWA web3 application and get the best features of TikTok, Instagram Reels, and YouTube Shorts.

Release Date: Presale starts on July, 2022

Category: NFT

CONTRACT INFO

Token Name
Cleeps

Symbol
CLPS

Contract Address
0xcbe24cAa3017B052280b41A66E066523e357a9dF

Network
Binance Smart Chain
TESTNET

Language
Solidity

Deployment Date
July 02, 2022

Verified?
Yes

Total Supply
180,000,000

Status
Not launched

TAXES

Buy Tax
none

Sell Tax
none

*Taxes cannot be changed

Our Contract Review Process

The contract review process pays special attention to the following:

- Testing the smart contracts against both common and uncommon vulnerabilities
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat

CURRENT STATS

(As of July 05, 2022)

Liquidity

Not added yet

Burn

No burnt tokens

Status:

Not Launched!

MaxTxAmount

No limit

DEX:

PancakeSwap

LP Address(es)

Liquidity not added yet

TOKEN TRANSFERS STATS

Transfer Count	Testnet deployment
Uniq Senders	Testnet deployment
Uniq Receivers	Testnet deployment
Total Amount	Testnet deployment
Median Transfer Amount	Testnet deployment
Average Transfer Amount	Testnet deployment
First transfer date	Testnet deployment
Last transfer date	Testnet deployment
Days token transferred	Testnet deployment

SMART CONTRACT STATS

Calls Count	Testnet deployment
External calls	Testnet deployment
Internal calls	Testnet deployment
Transactions count	Testnet deployment
Uniq Callers	Testnet deployment
Days contract called	Testnet deployment
Last transaction time	Testnet deployment
Created	Testnet deployment
Create TX	Testnet deployment
Creator	Testnet deployment

FEATURED WALLETS

Owner address	0x8cf4f5b619783694c9fb94a972186ce4c68788f3
LP address	**Not added yet**

TOP 3 UNLOCKED WALLETS

1 N/A TESTNET

2 N/A TESTNET

3 N/A TESTNET

VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

FOUND THREATS

⚠ Low

Owner can burn tokens from any address if there is enough allowance granted from the address.

```
function burnFrom(address from, uint amount) external onlyRole(BURNER_ROLE) {
    _spendAllowance(from, msg.sender, amount);
    _burn(from, amount);
}
```

FOUND THREATS

⚠ High Risk

No high risk-level threats found in this contract.

⚠ Medium Risk

Blacklist Function

- Owner can blacklist any address, making it impossible to sell.

```
function updateIsBot(address account, bool state) external onlyOwner {
    isBot[account] = state;
}

function bulkIsBot(address[] memory accounts, bool state) external onlyOwner {
    for (uint256 i = 0; i < accounts.length; i++) {
        isBot[accounts[i]] = state;
    }
}
```

- Recommendation:
  - Lorem ipsum dolor sit amet, consectetur adipiscing elit. Quisque libero nisl, consequat id malesuada eget, laoreet quis lacus. Vestibulum accumsan ex turpis, sed accumsan odio vulputate vitae. In quis lobortis ligula, a vehicula quam.

Informational

RECOMMENDATIONS FOR

GOOD PRACTICES

1. Consider fundamental tradeoffs
2. Be attentive to blockchain properties
3. Ensure careful rollouts
4. Keep contracts simple
5. Stay up to date and track development

Cleeps

GOOD PRACTICES FOUND

- ✔ The owner cannot mint new tokens after deployment
- ✔ The owner cannot stop or pause the contract
- ✔ The owner can set a transaction limit, but can’t lower it than 1% of total supply
- ✔ The smart contract utilizes "SafeMath" to prevent overflows

⚠️ There is currently no information about the initial tokens distribution based on the project's whitepaper and/or website.

THE TEAM

⚠️ The team is annonymous

KYC INFORMATION

⚠️ No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.

WEBSITE

Website URL
https://cleeps.io/

Domain Registry
https://www.namecheap.com/

Domain Expiration
Expires on 2023-02-21

Technical SEO Test
Passed

Security Test
Passed. SSL certificate present

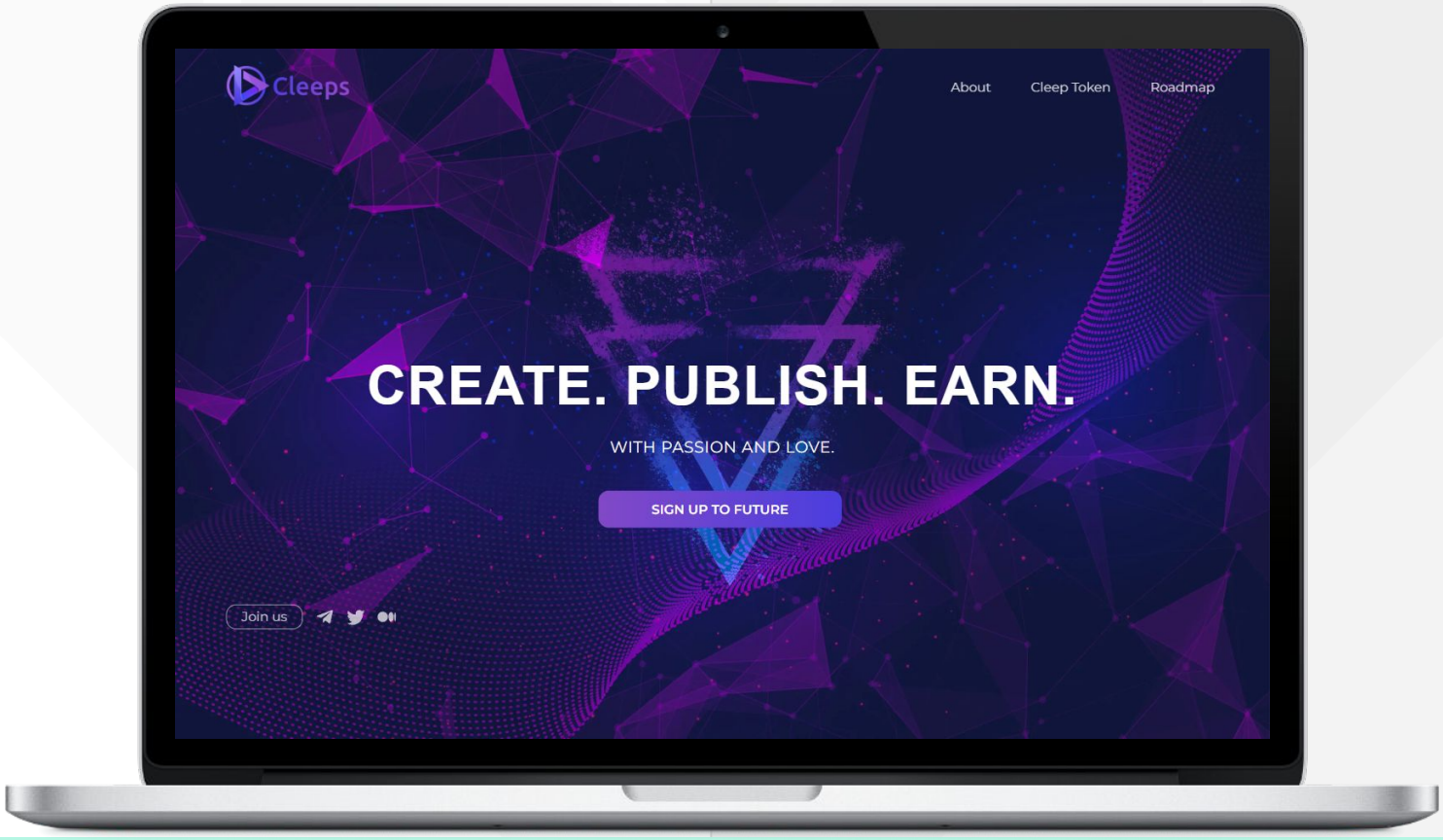
Design
Single page design, appropriate color scheme and graphics.

Content
The information helps new investors understand what the product does right away. No grammar mistakes found.

Whitepaper
Well written, explanatory, a bit short.

Roadmap
Yes, goals set with time frames.

Mobile-friendly?
Yes



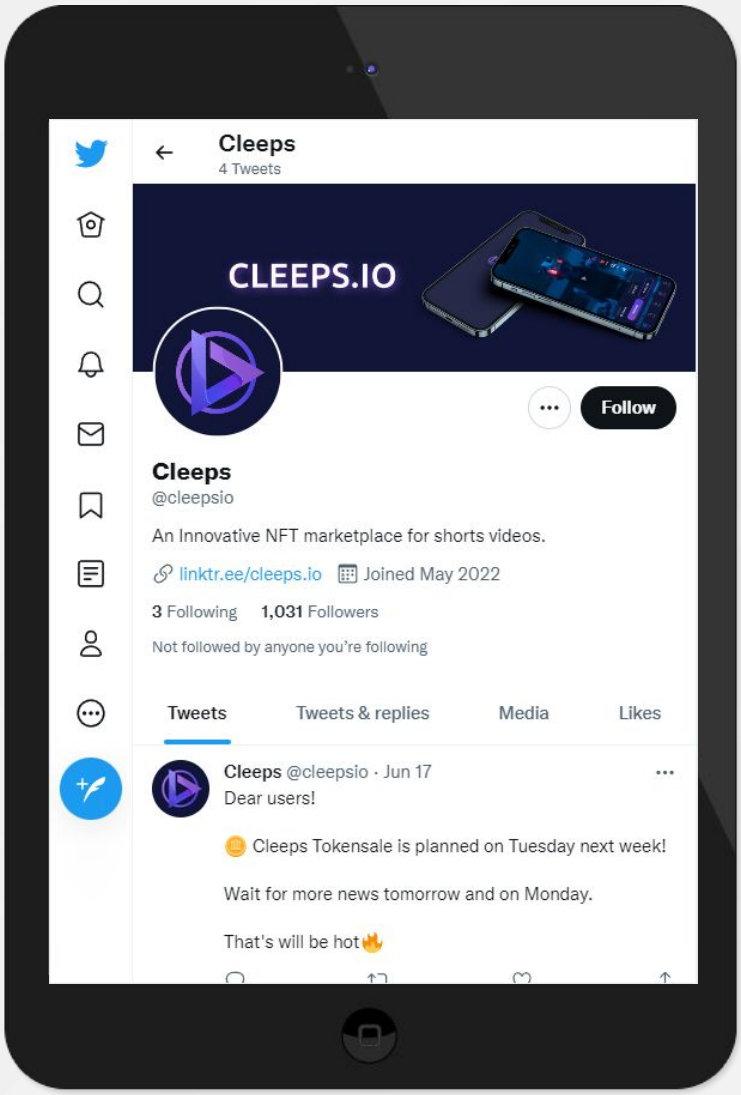
cleeps.io

SOCIAL MEDIA

& ONLINE PRESENCE

ANALYSIS

The project has low overall activity in social media. There were few posts and interactions, apparently, were interrupted in mid June.



Twitter

@cleepsio

- 1031 followers
- No tweets since June 17 (+15 days inactive)
- Few active followers

Discord

- Not available

Telegram

@cleeps_io

- 1046 members
- No messages since June 17 (+15 days inactive)

Medium

cleepsio.medium.com

- 1 follower
- No posts since June 9 (+15 days inactive)

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 150 SUCCESSFUL CLIENTS**
- **MORE THAN 500 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

SPYWOLF.NETWORK

@SPYWOLFNETWORK

@SPYWOLFOFFICIAL

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.